ты информации. В дальнейшем планируется продолжить расчеты многочленов больших степеней.

Библиографические ссылки

1. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М. : МЦНМО, 2004. 470 с.

2. *Лидл Р., Нидеррайтер Г.* Конечные поля : в 2 т. / пер. с англ. М. : Мир, 1988. Т. 1. 430 с.

3. *Демкина О. Е., Титов С. С., Торгашова А. В.* Рекуррентное вычисление неприводимых многочленов в задачах двоичного кодирования // Молодые ученые – транспорту : тр. IV науч.-техн. конф. Екатеринбург: УрГУПС, 2003. С. 391–404.

4. *Баданова О. М., Ициксон М. А., Титов С. С., Усольцев А. В.* Вычисление коэффициентов неприводимых делителей суммы геометрической прогрессии // Проблемы теоретической и прикладной математики : тр. 34-й регион. молодежной конф. Екатеринбург : УрО РАН, 2003. С. 3–4.

5. *Глуско К. Л., Титов С. С.* Арифметический алгоритм решения квадратных уравнений в конечных полях характеристики два // Докл. Том. гос. ун-та систем управления и радиоэлектроники. Томск : ТУСУР, 2012. № 1(25), ч. 2. С. 148–152.

АСИММЕТРИЧНЫЙ АЛГОРИТМ ШИФРОВАНИЯ

Н. Н. Гладков, М. А. Балашов, Т. Е. Иванов, С. С. Титов
(Екатеринбург, УрГУПС)

В наше время актуальной проблемой информационной безопасности является обеспечение безопасного обмена информацией между двумя пользователями. Одним из решений этой проблемы является использование алгоритмов шифрования, более надежными из которых являются асимметричные алгоритмы.

Асимметричный алгоритм шифрования – это алгоритм, использующий два математически связанных шифровальных ключа. Один ключ называется секретным и хранится в недоступном месте.

Другой ключ называется открытым и свободно предоставляется любым потенциальным пользователям.

Как правило, отправитель использует открытый ключ получателя для шифрования данных. Только получатель имеет связанный секретный ключ для расшифровки этого сообщения.

Одними из наиболее известных асимметричных алгоритмов являются RSA, ECC, алгоритм Диффи – Хеллмана. Наряду с ними можно рассмотреть алгоритм, использующий множество функций или неопределенные функции.

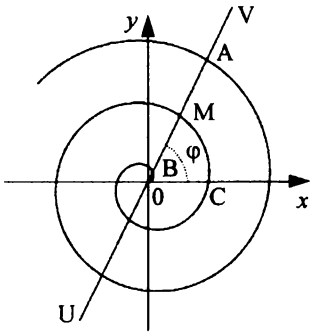
Суть этого алгоритма заключается в том, что одному значению из множества *X* соответствует множество значений *У* и одному значению из множества *У* соответствует множество значений *X*. Если рассматривать первый вариант, то публичным (открытым) ключом являются значения *У*, а секретным ключом – номер пересечения прямой, проходящей через значение *X*, параллельной оси *ОУ*, и функции.

Рассмотрим функции, которые можно использовать в данном алгоритме:

1. Спираль Архимеда.

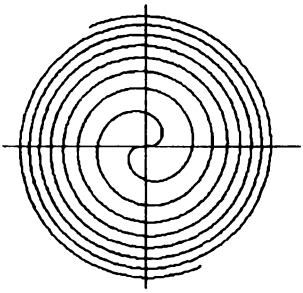
Архимедова спираль – плоская кривая, которую описывает точка, движущаяся равномерно-поступательно от центра О по равномерно-вращающемуся радиусу:

$$\rho = \alpha\varphi.$$



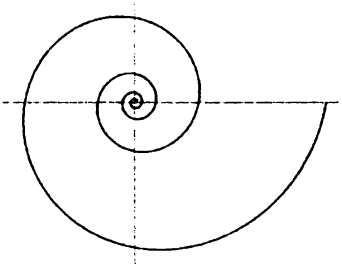
2. Спираль Ферма.

Спираль Ферма – спираль, задаваемая на плоскости в полярной системе координат уравнением $\rho = \alpha\sqrt{\varphi}$:



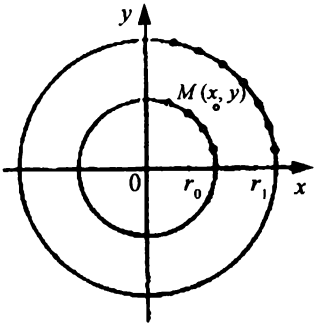
3. Логарифмическая спираль.

Логарифмическая спираль, или изогональная спираль, – плоская трансцендентная кривая, уравнение которой в полярной системе координат имеет вид $\rho = \alpha\varphi$, $\alpha > 0$:

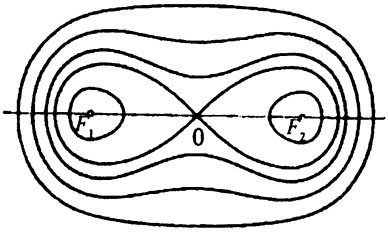


4. Множество окружностей.

Представлено множество окружностей, центр которых лежит в одной точке, а радиус увеличивается с заданным коэффициентом:



5. Лемниската – плоская алгебраическая кривая порядка $2n$, у которой произведение расстояний от каждой точки до n задаваемых точек постоянно:



Также к данным функциям можно отнести прямоугольную и квадратную спирали, спираль «жезл», гиперболическую спираль.

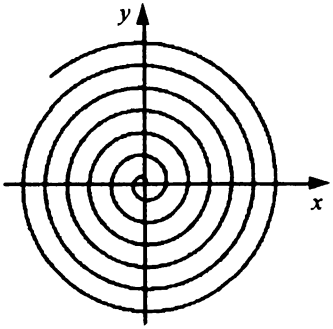
Рассмотрим принцип работы данного алгоритма:

1. Пользователи, совершающие обмен информации, устанавливают какое-то число – секретный ключ, которое равно номеру пересечения прямой, проходящей через значение X, параллельно оси OY и какой-либо функции.

2. Пользователь А, передающий информацию, указывает открытый ключ, состоящий из всех значений Y, в которых прямая пересекает функцию.

3. С помощью секретного ключа пользователь В узнает значение X, тем самым получая доступ к информации.

Рассмотрев функции и принцип работы данного алгоритма, представим пример. Для этого возьмем какую-нибудь неопределенную функцию, например, спираль:



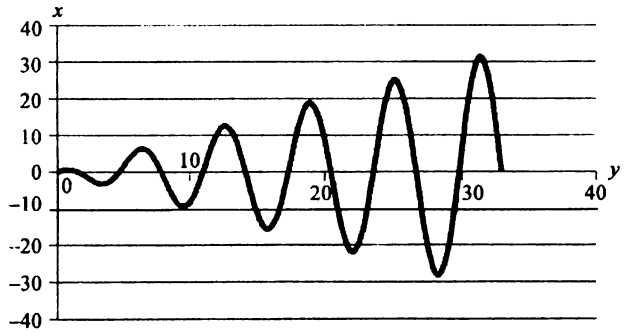
Представим функцию спирали $\rho = \alpha\varphi$ в декартовой системе координат:

$$\begin{cases} x = \rho\cos\varphi \\ y = \rho\sin\varphi. \end{cases}$$

В полярной системе координат эта функция представляет собой прямую, проходящую через начало координат с наклоном, зависящим от k. Предположим, что наша прямая проходит под углом 45°. Отсюда следует, что $\rho = \varphi$. Функция приобретает вид

$$\begin{cases} x = \varphi\cos\varphi \\ y = \varphi\sin\varphi. \end{cases}$$

Если представить эти формулы в виде графика, то получим следующее:



Из этого графика необходимо узнать величину, на которую увеличивается каждое колебание. Оно будет равно

$$\varphi_n \cos\varphi_n = x_0,$$

где $x_0 = K(\varphi_n)$.

$K(\varphi_n)$ – *уравнение Кеплера, которое используется в космонавтике.*

Таким образом, получаем, что величина, на которую увеличивается каждое колебание, зависит от коэффициента Кеплера. Получив ее, мы можем найти значения x и y.

Опишем весь алгоритм:

1. Пользователь А устанавливает какое-то конкретное значение x.

2. В зависимости от значения x с помощью формулы Кеплера определяется значение y.

3. Пользователь А отправляет значение y пользователю В.

4. Пользователь В, используя секретный ключ – конкретное пересечение, определяет значение x.

5. Пользователи А и В получают доступ к информации.

Из этого следует, что другие пользователи, не зная секретного ключа, не имеют доступа к передаваемой информации. Вся сложность данного алгоритма заключается в бесконечно большом количестве значений, в которых происходит пересечение. Другие пользователи, не зная секретного ключа, не имеют доступа к передаваемой информации. Следовательно, данный алгоритм может использоваться как алгоритм защиты передаваемой информации между двумя пользователями.

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

В. В. Егоров
(Екатеринбург, УрФУ, evv93@mail.ru)

Целью прохождения практики на предприятии являлось ознакомление и изучение средств защиты персональных данных от несанкционированного доступа (НСД). Особое внимание было уделено средствам защиты информации, в основе которых лежат принципы использования криптографии, использование этих средств на предприятии.

Криптография в прошлом использовалась лишь в военных целях. Однако сейчас, по мере образования информационного общества, она становится одним из основных инструментов, обеспечивающих конфиденциальность, доверие, авторизацию, электронные